REMARKS

Upon entry of this Response, claims 1-3, 5-10, 12-18, and 20-23 remain pending in the present patent application. Claims 4, 11, and 19 have been canceled herein. No amendments are presented herein, where the claims are listed for the sake of convenience. Applicants respectfully request reconsideration of the pending claims in view of the following remarks.

In item 6 of the Office Action, claims 1, 6, 9, 13, 16, and 21 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent 6,446,204 issued to Pang et al. (hereafter "*Pang*"). Anticipation under §102 "requires the disclosure in a single prior art reference of each element of the claim under construction. W.L. Gore & Associates, Inc. v. Garlock, Inc., 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983). For the reasons that follow Applicant asserts that the rejection of claims 1, 6, 9, 13, 16, and 21 as being anticipated by *Pang* is improper. Accordingly, Applicant requests that the rejection of these claims be withdrawn.

To begin, claim 1 as previously amended recites as follows:

> 1. A system for authentication, comprising:
>   a processor circuit having a processor and a memory;
>   an authentication system stored in the memory and executable by the processor, the authentication system comprising:
>   a plurality of authentication agents, each of the authentication agents authenticating at least one user parameter by performing at least one authentication task; and
>   an authentication manager that requests each of the authentication agents to authenticate an unauthenticated user parameter until all of the authentication agents have been requested to authenticate the unauthenticated user parameter and the authenticated user parameter is authenticated by at least one of the authentication agents, unless one of the authentication agents fails to authenticate the unauthenticated user parameter.

As set forth in claim 1 above, the authentication manager requests each of the authentication agents to authenticate an unauthenticated user parameter until all of the authentication agents have been requested to authenticate **the** authentication parameter and the authenticated user parameter is authenticated by at least one of the

authentication agents. Such is the case unless one of the authentication agents fails to authenticate the unauthenticated user parameter.

Given that each of the authentication agents is requested to authenticate **the unauthenticated** parameter, claim 1 thus specifies that all of the authentication agents are requested to authenticate the same unauthenticated user parameter. This is the case even if the authentication agents may be configured to authenticate parameters of a different type than the unauthenticated user parameter, where some of the authentication agents do not operate to authenticate various types of authentication parameters that they may be requested to authenticate.

This fact facilitates the extensibility of the design of the authentication system according to the present invention. In particular, authentication agents can receive a request to authenticate a user parameter that they are not configured to authenticate. In such situations, the authentication agents simply transmit a "valid" reply back to the authentication manager and the authentication manager will not know that the authentication agent was not actually configured to authenticate the type of parameter it was asked to do. In this respect, authentication agents may more easily be added to the authentication system without worrying about trying to map given types of authentication parameters to be sent to specific ones of the authentication agents for authentication.

In contrast, *Pang* describes in the process of FIG. 7A and 7B the authentication of individual user parameters by sending specific parameters to specific authentication agents that are configured to authenticate those given parameters. In other words, no one authentication parameter is supplied to all of the authentication agents ("Providers") of *Pang*. Specifically, the provider 606 receives the name of a given individual as an authentication parameter to authenticate, and the provider 608 is given an IP address to authenticate. It is not the case, for example, that the IP address is given to both the providers 606 and 608.

Thus, the Providers must be statically linked to the authentication manager software of *Pang* in order to route the proper types of authentication parameters to the corresponding ones of the authentication agents. In contrast, to add new types of user parameters for authentication according to the claimed embodiments of the present

- 12 -

invention, agents may simply be added to the system without regard for trying to map static links between the agents and the manager.

Therefore, Applicants assert that *Pang* fails to show or suggest each of the elements of claim 1 as previously amended. Also, Applicants assert that *Pang* fails to show or suggest each of the elements of claims 9 and 16, to the extent that these claims incorporate subject matter similar in scope with that of claim 1. Accordingly, Applicants request that the rejection of claims 1, 9, and 16 be withdrawn. In addition, Applicants request that the rejection of claims 6, 13, and 21 be withdrawn as depending from claims 1, 9, or 16, respectively.

Next, in item 7 of the Office Action, claims 2, 7-8, 14-15, 17, and 22-23 have been rejected under 35 U.S.C. §103(a) as being unpatentable over *Pang*. A prima facie case of obviousness is established only when the prior art teaches or suggests all of the elements of the claims. MPEP §2143.03, In re Riickaert, 9 F.3d 1531, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). For the reasons that follow, Applicants assert that the rejection of claims 2, 7-8, 14-15, 17, 22-23 are improper. Accordingly, Applicants request that the rejection of these claims be withdrawn.

To begin, claim 2 as previously amended states as follows:

> 2.   The system of claim 1, wherein the authentication manager waits for a response from each of the authentication agents, each response indicating whether the unauthenticated user parameter has been authenticated.

With respect to claims 2 and 17, the Office Action states in part:

> "Pang et al. do not expressly disclose wherein the authentication manager waits for a response from each of he authentication agents. However, Pang et al. disclose the request may be removed from the waiting list and the message may be sent to the browser to indicate that the request cannot be processed if the request stayed on the waiting list for a predetermined amount of time **[If the revised browser request remains on the waiting list for more than a predetermined amount of time, listener 210 may remove the request from the waiting list and send a message to the browser 202 to indicate that the request could not be processed (lines 60-64, Col. 16)]**. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Pang et al. to have the predetermined-waiting-time feature incorporated into the authentication process since one would have

- 13 -

been motivated to increase the efficiency of the application server (line 9, Col. 13 from Pang et al.) by imposing an additional restriction on the authentication response waiting time." (Office Action, pages 11-12.)

Applicants respectfully disagree with the above assertion. In particular, at lines 60-64 of column 16, *Pang* describes the operation of a web application server and the processing of browser requests. They are not the same as authentication requests as set forth in claim 2 above.

In addition, the statement that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify *Pang* et al. to have the predetermined waiting time feature incorporated into the authentication process since one would have been motivated to increase the efficiency of the application server by imposing an additional restriction on the authentication response waiting time" makes no since in light of the fact a wait does not increase efficiency. In particular, the authentication manager as set forth in claim 2 waits to receive a response from each one of the authentication agents as a given item will not be authenticated until all agents have responded to a given request provided to them for a single given parameter. If any one of the agents is not configured to authenticate the parameter which is the subject of a given request, then such agents simply reply back to the authentication manager that the parameter is "valid" or provide some other designation, thereby causing the manager to believe that the specific parameter was authenticated.

It is by using this approach that benefits are realized to the extent that additional authentication agents may be added that need not be statically linked to the authentication manager as was described above. The statement that one would have been motivated to increase the efficiency of the application server by imposing an additional restriction on the authentication response waiting time makes no since as one would not be motivated to increase the response waiting times, rather one would be motivated to reduce such waiting times for authentication. It just so happens that the individual authentication agents do not delay the process in authenticating a parameter if they are configured to authenticate a parameter of a given type. Rather, such agents simply respond with a "valid" response or other appropriate response.

- 14 -

Accordingly, Applicants assert that the rejection of claim 2 is improper. Also, Applicants assert that the rejection of claim 17 is improper to the extent that claim 17 includes subject matter similar in scope with that of claim 2. Accordingly, Applicant requests that the rejection of claims 2 and 17 be withdrawn.

Next, claim 7 as previously amended provides as follows:

> 7.   A system for authentication, comprising:
> a processor circuit having a processor and a memory;
> an authentication system stored in the memory and executable by the processor, the authentication system comprising:
> a plurality of authentication agents, each of the authentication agents authenticating at least one user parameter by performing at least one authentication task;
> an authentication manager that requests each of the authentication agents to authenticate an unauthenticated user parameter; and
> wherein, upon startup, the authentication manager is unaware of how many of the authentication agents exist in association with the authentication system and the authentication manager discovers the authentication agents.

As set forth above, claim 7 specifies that the authentication manager is unaware of how many authentication agents exist in association with the authentication system upon startup when the authentication manager discovers the authentication agents. With respect to at least this element of claim 7, the Office Action states as follows:

> "Pang et al. do not expressly disclose wherein, upon startup, the authentication manager is unaware of how many of the authentication agents exist in association with the authentication system and the authentication manger discovers the authentication agents. However, Pang et al. disclose the providers are implemented as dynamically linked libraries (DLLs) and loaded dynamically at the runtime only and the communication of is through the use of Microsoft COM or remote procedure calls (RPC) [**Providers are implemented as dynamically linked libraries (DLLs). As such, the providers are loaded into and execute within the same address space as the authentication hosts to which they belong (lines 1-4, Col. 20). The providers are preferably loaded dynamically at run time (lines 4-5, Col. 20). For example, the components of web application server 280 may alternatively communicate with each other using Remote Procedure Calls (RPC), a UNIX, Microsoft COM (lines 64-67, Col. 17**); *where dynamically links at the running time only means the exact number of agents are unknown prior to the process is running*]. Therefore, It would have been obvious to one of ordinary

- 15 -

skill in the art at the time of invention was made to modify that Pang et al. to have the discovery procedure of the provider specified since one would be motivated to have a mechanism which allows providers to be dynamically added and removed from the authentication server (lines 22-24, Col. 20 from Pang et al.). Thus, it would have been obvious to modify Pang et al. to obtain the invention as specified in claim 7." (Office Action, pages 14-15.)

Applicants respectfully disagree. Specifically, operative within the terms "dynamically linked libraries" is the term "linked". In this respect, the link is a specific static link between the various providers included in the library and the given authentication host as described by *Pang*. In particular, a dynamically linked library is a feature of the Microsoft Windows™ family of operating systems and OS/2 that allows executable routines to be stored separately as filed with DLL extensions **and to be loaded only when needed by a program**. A dynamically linked library file has advantages in that it does not consume any memory until it is used, and, because a dynamically linked library is a separate file, a programmer can make corrections or improvements to only that module without affecting the operation of the calling program or any other dynamically linked library. Also, dynamically linked libraries may be reused with other programs.

Although a dynamic linked library has advantages as described above, there is still a static link between the providers of the dynamically linked library and the authentication host. The only difference is that the providers are loaded and executed when called as opposed to being loaded and executed when the authentication host is loaded and executed. Thus, a link must exist between the authentication host and the given providers or they could not be called up and executed during run time.

Since a static link does exist between the authentication host and the given providers and stored as a dynamically linked library as set forth in *Pang*, it is not the case that *Pang* shows or suggests that upon start the authentication manager is unaware of how many of the authentication agents exist in association with the authentication system and that the authentication manager discovers the authentication agents. Rather, the static links between the providers and the authentication host of

- 16 -

Application Number: 10/060,780   Docket Number: 10012156-1

Pang ensures that the authentication host can access the providers when needed. In this respect, the authentication host is aware of the existence of the providers.

Accordingly, Applicants assert that *Pang* fails to show or suggest each of the elements of claim 7 as it currently stands. In addition, Applicants assert that *Pang* fails to show or suggest each of the elements of claims 14 and 22 to the extent that they include subject matter similar in scope with that of claim 7. Accordingly, Applicants request that the rejection of claim 7, 14, and 22 be withdrawn. In addition, Applicants respectfully requests that the rejection of claims 8, 15, and 23 be withdrawn as depending from claim 7, 14, and 22, respectively, for the reasons described above with reference to claim 7, 14, and 22.

In item 8 of the Office Action, claims 4-5, 11-12, and 19-20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over *Pang*, and further in view of U.S. Patent 6,615,264 issued to Stoltz et al. (hereafter "*Stoltz*"). A prima facie case of obviousness is established only when the prior art teaches or suggests all of the elements of the claims. MPEP §2143.03, In re Rijckaert, 9 F.3d 1531, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). Claims 4, 11, and 19 have been canceled herein, thereby rendering this rejection moot with respect to such claims. Applicants assert that the cited combination of references fails to show or suggest each of the elements of claims 5, 12, and 20. Accordingly, Applicants respectfully requests rejection of claims 5, 12, and 20 be withdrawn. To begin, claim 5 as previously amended provides as follows:

- 17 -

5.   A system for authentication, comprising:
a processor circuit having a processor and a memory;
an authentication system stored in the memory and executable by the processor, the authentication system comprising:
a plurality of authentication agents, each of the authentication agents authenticating at least one user parameter by performing at least one authentication task, wherein a parameter type associated with each of the authentication agents; and
an authentication manager that requests each of the authentication agents to authenticate an unauthenticated user parameter
wherein each of the authentication agents authenticates the unauthenticated user parameter if the unauthenticated user parameter is of the parameter type associated with the respective authentication agent; and
wherein:
each of the authentication agents transmits an invalid response to the authentication manager upon a failure to authenticate the unauthenticated user parameter;
each of the authentication agents transmits a valid response to the authentication manager upon a successful authentication of the unauthenticated user parameter; and
each of the authentication agents transmits a valid response to the authentication manager if the unauthenticated user parameter is of a parameter type that is different than the parameter type associated with the respective authentication agent.

With respect to claim 5, the Office Action states:

"Pang et al. do not expressly disclose each of the authentication agents transmits a valid response to the authentication manager if the unauthenticated user parameter is of a parameter type that is different than the parameter type associated with the respective authentication agent. However, Stoltz et al. disclose plurality of authentication modules and each has the option of accepting or declining responsibility for a request such that it can accept all the request at all the time, part of the time, or not accepting the request at all [Authentication modules 240 each have the option of accepting or declining responsibility for a particular connection. Authentication modules 240 may base their decision on other available system resources or settings (e.g., from services 230-238, external databases, etc.). In one or more embodiments, an authentication module 240 can be configured to accept all users

- 18 -

Application Number: 10/060,780   Docket Number: 10012156-1

all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example (lines 57-t65, Col. 8); *where declining can be due to the reason, such as the field of authentication is not the right type associated with the module].*" (Office Action, pages 29-30.)

Applicants respectfully disagree. Specifically, at column 8, lines 57-65, *Stoltz* states as follows:

"Authentication modules **240** each have the option of accepting or declining responsibility for a particular connection. Authentication modules **240** may base their decision on other available system resources or settings (e.g., from services **230-238**, external databases, etc.). In one or more embodiments, an authentication module **240** can be configured to accept all users all of the time, to only accept connections with smart cards, or to only accept users with pseudo tokens, for example."

Thus, authentication modules as taught by *Stoltz* have the option of accepting or declining responsibility for a particular connection. However, in declining responsibility for connection, the authentication modules of *Stoltz* do not transmit a "valid" response to the authentication manager. Due to the fact that the agents transmit a "valid" response in such circumstances, the authentication manager is of lesser complexity and does not have to deal with a greater number of potential responses from the agents. Also, this feature further facilitates the easy addition of new agents to the authentication system without creating further static connections with the authentication manager.

Accordingly, Applicants assert that the rejection of claims 5, 12, and 20 is improper. Accordingly, Applicants request that the rejection of claims 5, 12, and 20 be withdrawn.

In addition, in item 9 of the Office Action, claims 3, 10, and 18 have been rejected under 35 U.S.C. §103(a) as being unpatentable over *Pang* as applied to claims 1, 9, and 16, and further in view of U.S. Patent Publication 2002/0069247 filed by Paknad et al. (hereafter "*Paknad*"). A prima facie case of obviousness is established only when the prior art teaches or suggests all of the elements of the claims. MPEP §2143.03, In re Rijckaert, 9 F.3d 1531, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). Applicants note that claims 3, 10, and 18 depend from claims 1, 9, and 16. Accordingly, Applicants assert that the cited combination of references fail to show or suggest each of the

- 19 -

elements of claims 3, 10, and 18 as depending from claims 1, 9, and 16 for the reasons described above. Accordingly, Applicants request that the rejection of claims 3, 10, and 18 be withdrawn.

CONCLUSION

Applicants respectfully request that all outstanding objections and rejections be withdrawn and that this application and all presently pending claims be allowed to issue. If the Examiner has any questions or comments regarding this response, the Examiner is encouraged to telephone the undersigned counsel of Applicants.

Respectfully submitted,

Michael J. D'Aurelio
Reg. No. 40,977

Thomas, Kayden, Horstemeyer
& Risley, L.L.P.
100 Galleria Parkway, N.W.
Suite 1750
Atlanta, Georgia 30339-5948
Phone: (770) 933-9500
Fax   (770) 951-0933

BEST AVAILABLE COPY

- 20 -